

Windows Mobile 6 Wireless Tests ("After" Example)

Introduction

NOTE: This document only presents the public portions of the relevant test documentation. The public portions are shared with Windows Embedded CE, and are available on MSDN as part of the Windows Embedded CE help content.

Table of Contents

Wi-Fi Tests

- Wi-Fi Authentication Tests
 - Wi-Fi Authentication Tests Overview
 - Prerequisites for the Wi-Fi Authentication Tests
 - Establishing the Correct Test Environment for Wi-Fi Authentication Tests
 - ▽ How to Set Up the Windows Mobile Authentication Servers on Windows Server 2003
 - ▽ How To Set Up Active Directory
 - ▽ How To Set Up a DNS Server
 - ▽ How To Set Up a DHCP Server
 - ▽ How to Set UP Internet Information Services
 - ▽ How To Set Up the Internet Authentication Service
 - ▽ How To Set Up the AP Control Server
 - ▽ How To Set Up RADIUS Clients
 - ▽ How To Set Up Certificate Services
 - ▽ How To Enable Certificate Templates
 - ▽ How To Create User Groups and Remote Accounts
 - ▽ How To Create Remote Policies by Using IAS
 - ▽ Verifying the Test Environment for Wi-Fi Authentication Tests
 - ▽ How To Configure Wi-Fi Authentication Access Points
 - Running the Wi-Fi Authentication Tests
 - ▽ Example Test Configurations for the Wi-Fi Configuration Tests
 - Command Line Parameters for the Wi-Fi Authentication Tests
 - ▽ AP Control Server Settings for the Wi-Fi Authentication Tests
 - ▽ Certificate Enrollment Settings for the Wi-Fi Authentication Tests
 - ▽ User Log-on Settings for the Wi-Fi Authentication Tests
 - ▽ Authentication Test Settings for the Wi-Fi Authentication Tests
 - Test Cases for the Wi-Fi Authentication Tests
 - ▽ Open Authentication Test Cases
 - ▽ Shared Authentication Test Cases
 - ▽ WEP 802.1x Authentication Test Cases
 - ▽ WPA Authentication Test Cases
 - ▽ WPA-PSK Authentication Test Cases

- ▽ WPA2 Authentication Test Cases
- ▽ WPA2-PSK Authentication Test Cases
- Troubleshooting the Wi-Fi Authentication Tests

Wi-Fi Tests



8/27/2008

This section contains documentation for Windows Embedded CE 6.0 Test Kit (CETK) tests that exercise the Wi-Fi hardware and drivers on the target device.

In This Section

[Wi-Fi Authentication Tests](#)

Describes how to set up and run the automated tests necessary to verify Wi-Fi authentication functionality.

See Also

Other Resources

[CETK Tests](#)

Wi-Fi Authentication Tests



8/27/2008

For a Windows Mobile powered device that connects to a network in infrastructure mode, the tests in the Wi-Fi Authentication Test Suite validate proper operation by exercising all valid combinations of the authentication and encryption protocols for the device in relation to an access point (AP). Additionally, these tests help ensure that the Windows Mobile powered device does not connect to an AP when the configuration is incorrect.

Passing the Wi-Fi Authentication Test is a requirement for a Windows Mobile powered device to receive logo certification.

In This Section

[Wi-Fi Authentication Tests Overview](#)

Provides a conceptual diagram of the network architecture, as well as an overview of the encryption and authentication methods and a general description of the processes within the test.

[Establishing the Correct Test Environment for Wi-Fi Authentication Tests](#)

Provides detailed information about how to set up the test environment.

[Running the Wi-Fi Authentication Tests](#)

Explains how to run the test.

[Test Cases for the Wi-Fi Authentication Test](#)

Describes the test cases found in this test.

[Command Line Parameters for the Wi-Fi Authentication Tests](#)

Specifies the command-line parameters that can be used with this test.

[Troubleshooting the Wi-Fi Authentication Tests](#)

Provides troubleshooting help for this test.

See Also

Other Resources

[Wi-Fi Tests](#)

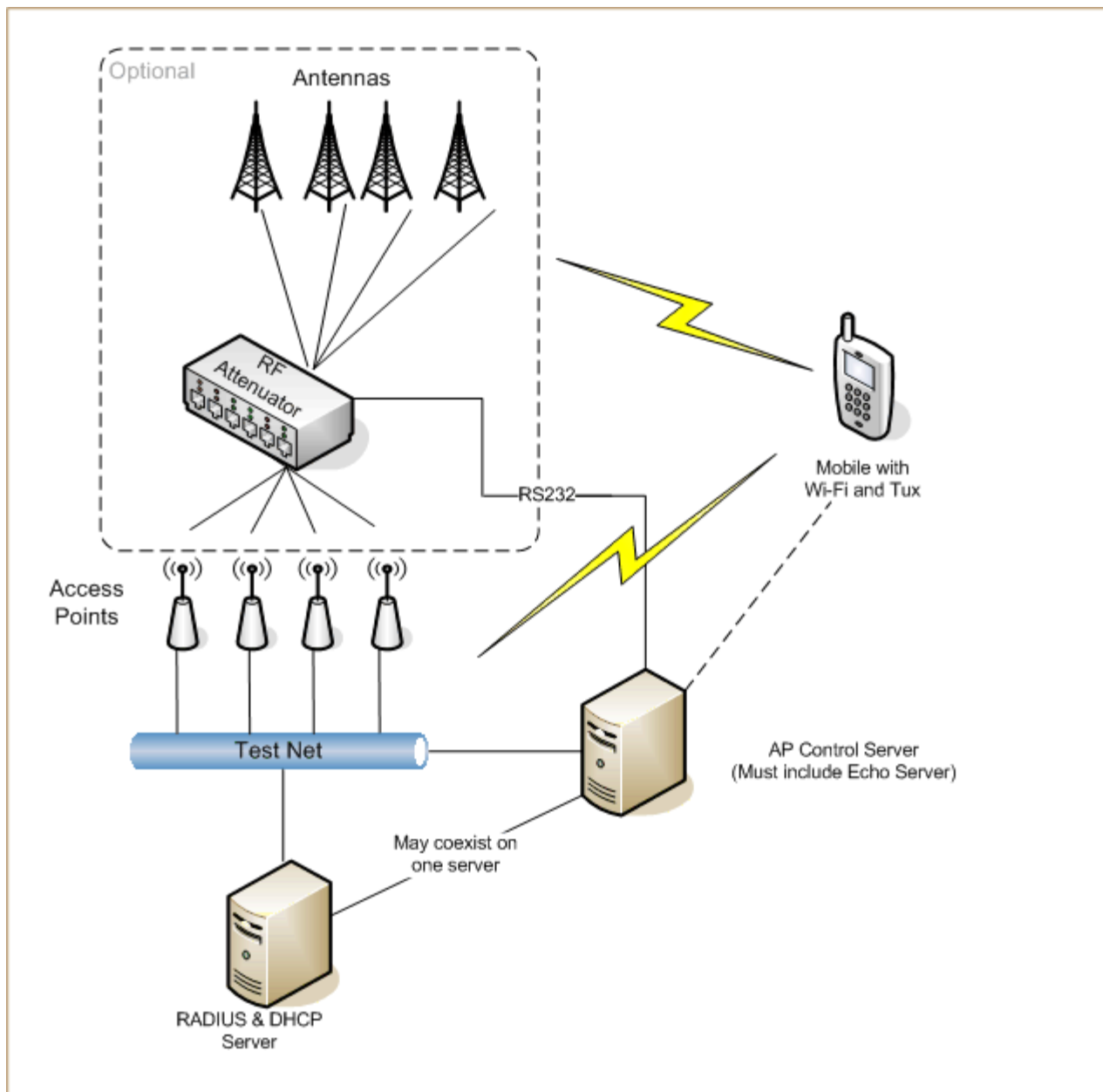
Wi-Fi Authentication Tests Overview



Writing Sample--Windows Mobile Wireless Tests—"After" Example
Katy Koenen

To validate that a Wi-Fi station can connect to the appropriate access point (AP) through each valid combination of authentication and encryption protocols, you must test all of these connections. In addition, you must test to ensure that a Windows Mobile powered device does not connect to any AP for which the device is not configured.

The Wi-Fi Authentication Tests requires three servers: the AP Control server, the Remote Authentication Dial-in User Service (RADIUS) server (commonly known as the Authentication Authorization Accounting (AAA) server), and the Dynamic Host Control Protocol (DHCP) server. You can choose to install all of these servers on the same computer, or you can install them on separate computers. The following illustration shows an example of a test network configuration.



The AP Control server handles access point configuration requests from the device that is being tested and updates the APs to the required security modes. This server must run both the UDP and TCP Echo services to allow the device to verify a wireless connection.

The RADIUS server stores a list of clients, that is, the access points which connect to it. This list must include each access point that the device supports. The list entry for each access point client also contains a secret pass phrase the clients use to communicate with the RADIUS server. Enter a pass phrase for each access point, and then configure the keys for the corresponding APs so that they can be authenticated by the RADIUS server during EAPOL key processing. If the RADIUS server is also the authentication server,

which is usually the case, this server must have two special user accounts: one for Transport Layer Security (TLS) Extensible Authentication Protocol (EAP) authentication, and one for the Protected Extensible Authentication Protocol (PEAP). The tests default to the following credentials for these accounts:

TLS authentication

- User name: eaptls
- Password: eaptls
- Domain: wince

PEAP authentication

- User name: eappeap
- Password: eappeap
- Domain: wince

The DHCP server provides a framework for passing configuration data to devices in a TCP/IP network, which eliminates the problems associated with manual configuration. When a DHCP server receives a request, the server automatically assigns an IP address from a pool of addresses, as well as assigning the address mask, the default gateway, the DNS server, the domain name, the WINS server (if used), and so on, to the device or computer that made the request.

The Wi-Fi Authentication tests run a variety of authentication and encryption methods to validate Wi-Fi functionality for a Windows Mobile powered device, as shown in the table that follows.

General authentication methods

| Authentication method | Description |
|-----------------------|--|
| Open | All associations are accepted. |
| Shared | All associations are accepted, but the client must use WEP encryption. |
| WPA | Wi-Fi Protected Access. Requires EAP authentication. |
| WPA-PSK | WPA with a pre-shared key (PSK). |
| WPA2 | Wi-Fi Protected Access 2. Requires EAP authentication. |
| WPA2-PSK | WPA2 with PSK. |

EAP authentication methods

- Transport Layer Security (TLS)
- Message Digest 5 (MD5)
- Protected Extensible Authentication Protocol (PEAP)

Encryption methods

- Unencrypted (Clear Text)
- Wired Equivalent Privacy (WEP)
- Temporal Key Integrity Protocol (TKIP)
- Advanced Encryption Standard (AES)

For each combination of authentication and encryption protocols, the test performs the following steps:

1. Connects with an AP control server by using a fixed-configuration access point.
2. Requests the AP control server to configure an access point with a given authentication, encryption, and key.
3. Disconnects from the fixed-configuration access point.

4. Configures the device being tested to the so that it will connect to the access point that was configured in step 2 with the specified SSID, authentication method, encryption method, and key being tested.
5. Waits for a fixed interval for the connection to be established.
6. Sends a large number of ICMP pings through the newly-connected Wi-Fi link and checks for an equal number of replies.
7. Sends a large number of UDP echoes, and checks for lost or corrupted replies.
8. Sends a large number of TCP echoes, and checks for lost or corrupted.
9. Disconnects the wireless adapter.

The Wi-Fi Authentication Test is implemented as a Tux DLL. It can be started and configured remotely by using either CETK or Platform Builder , or locally by using a command script.

See Also

Tasks

[Establishing the Correct Test Environment for Wi-Fi Authentication Tests](#)

Other Resources

[Wi-Fi Authentication Tests](#)

Prerequisites for the Wi-Fi Authentication Tests



8/27/2008

The following table shows the hardware requirements for the Wi-Fi Authentication Test.

| Requirement | Description |
|-------------------------|--|
| Device under test | The Windows Embedded CE-based device or devices you want to test. |
| Fixed access point (AP) | This AP must not require 802.1X (EAP) authentication; that is, it must require Open, Shared, WPA-PSK or WPA2-PSK authentication. The device(s) under test use this AP to request AP test reconfiguration through the AP control server. |
| One or more APs | Every AP is controllable, and will be reconfigured during the testing by the AP control server. Each AP must be configured to communicate with the RADIUS authentication server. |
| Control server for APs | Processes AP configuration requests from the devices under test and updates APs to the required security mode. This server must also run the UDP and TCP Echo services so that the device(s) under test can verify wireless connections. |
| RADIUS server | Authentication server. You can run this service on its own computer, or on a computer that also runs the AP control server and the DHCP server. |
| DHCP server | Assigns IP addresses and processes client requests. You can run this server on its own computer, or on a computer that also runs the authentication and AP control servers. |
| Local network | Subnet to which the AP server, RADIUS server, and DHCP server all connect, so that the device can contact each server. |

The following table shows the software requirements for the Wi-Fi Authentication Matrix Test.

| Requirement | Description |
|---|--|
| Windows Server 2003, any of the Standard or Enterprise editions | Basic server software requirement for running the Wi-Fi Authentication Test Suite. |
| Tux.exe | Test harness; required to run the tests. |
| Kato.dll | Logging engine, required to log data. |
| Authmatrix.dll | Test library. |

| | |
|---------------|--|
| Apcontrol.exe | Runs the AP control server. |
| Enroll.exe | Retrieves security certificate from the server that provides authentication services for the test network. |
| Netall.dll | Provides networking utilities; must reside on both the client and server. |

See Also

Other Resources

[How To Set Up the Windows Mobile Authentication Servers on Windows Server 2003](#)

[Wi-Fi Authentication Tests](#)

Establishing the Correct Test Environment for Wi-Fi Authentication Tests



8/27/2008

The following table describes the steps that are necessary to create an appropriate test environment for running the Wi-Fi Authentication tests and, thus, validate the Wi-Fi functionality of the device.

Procedure

To set up the test environment

1. Confirm that you have carefully read the list of all the prerequisites and that all of the hardware and software requirements are met. For more information, see [Prerequisites for the Wi-Fi Authentication Tests](#).
2. Set up the authorization servers on a computer that is running the Windows Server 2003 operating system. For more information, see [How To Set Up the Windows Mobile Authentication Servers on Windows Server 2003](#).
3. Create a private network by connecting the access points and devices being tested to the computer hosting the servers.

Important:

To ensure that all devices on your test network have valid and unique IP addresses, the test network must be isolated and private. Make sure that the test network is not connected to the corporate network.

4. Check to make sure that your private network is properly configured and that the static and dynamic IP addresses are properly assigned. For more information, see [Verifying the Test Environment for Wi-Fi Authentication Tests](#).
5. After you have confirmed that your test network is set up correctly, you can begin running the Wi-Fi Authentication Test.

See Also

Tasks

[How To Configure Wi-Fi Authentication Access Points](#)

[Running the Wi-Fi Authentication Tests](#)

Other Resources

[Wi-Fi Authentication Tests](#)

How To Set Up the Windows Mobile Authentication Servers on Windows Server 2003



8/27/2008

Verifying the Wi-Fi functionality of a Windows Mobile powered device requires a test environment that includes a private network that contains various authentication servers. The following topics describe how to install and configure those authentication servers to support the Wi-Fi Authentication test environment.

In This Section

[Prerequisites for the Wi-Fi Authentication Tests](#)

Writing Sample--Windows Mobile Wireless Tests—"After" Example
Katy Koenen

Describes the hardware and software necessary to set up the necessary test environment.

[How To Set Up Active Directory](#)

Describes how to set up Active Directory.

[How To Set Up a DNS Server](#)

Describes how to set up a Domain Name server.

[How To Set Up a DHCP Server](#)

Describes how to install and configure a DHCP server.

[How To Set Up Internet Information Services](#)

Describes how to install Internet Information Services (IIS).

[How To Set Up the Internet Authentication Service](#)

Describes how to set up the Internet Authentication Service (IAS).

[How To Set Up the AP Control Server](#)

Describes how to install and configure an AP Control server.

[How To Set Up RADIUS Clients](#)

Describes how to set up RADIUS server clients.

[How To Set Up Certificate Services](#)

Describes how to install and configure Certificate Services.

[How To Enable Certificate Templates](#)

Describes how to enable certificate templates.

[How To Create User Groups and Remote Accounts](#)

Describes how to set up user groups and remote accounts.

[How To Create Remote Policies by Using IAS](#)

Describes how to set up remote policies by using the Internet Authentication Service (IAS).

See Also

Tasks

[Establishing the Correct Test Environment for Wi-Fi Authentication Tests](#)

Other Resources

[Wi-Fi Authentication Tests](#)

How To Set Up Active Directory



8/27/2008

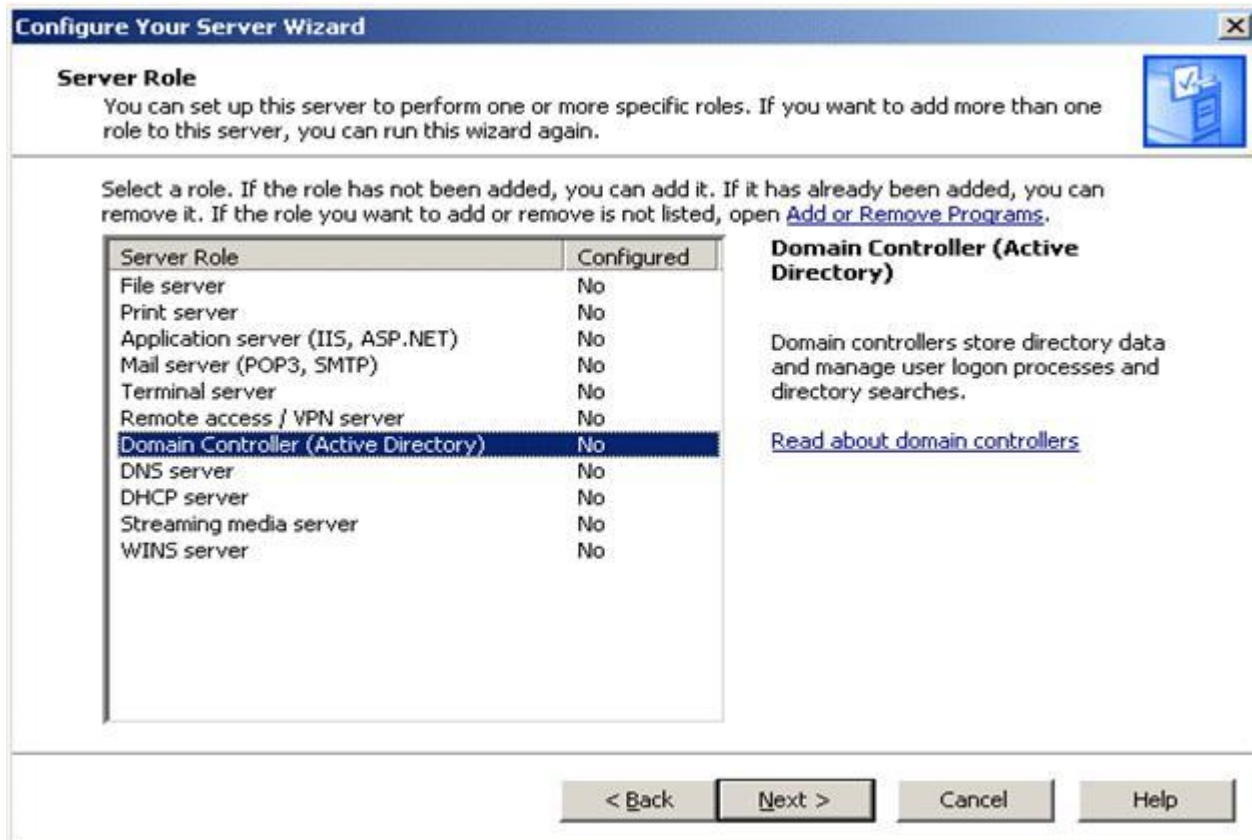
When you install Windows Server 2003 and log in for the first time, the **Manage Your Server** window opens.

Procedure

To configure Active Directory

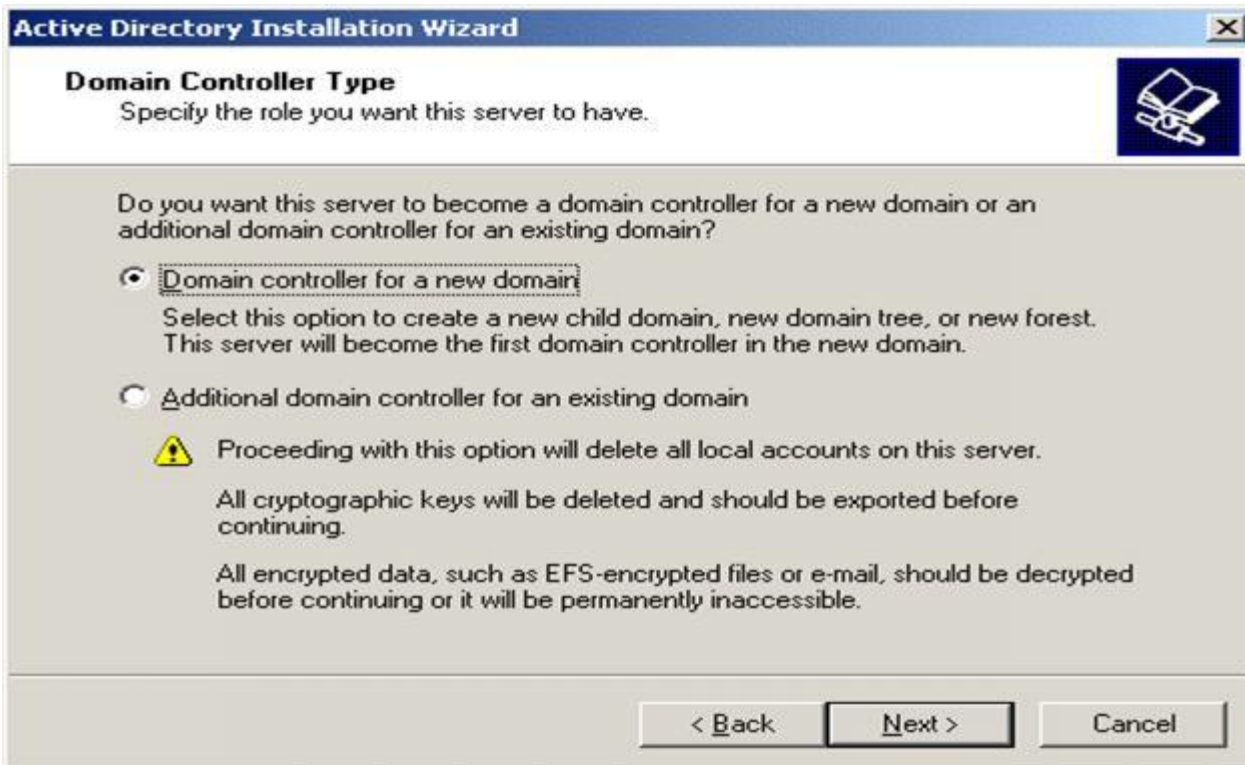
1. In the **Manage Your Server** window, click the **Add or remove a role** icon, which will open the Configure Your Server Wizard.
2. On the **Preliminary Steps** page, make sure that you have completed all of the prerequisite preparation, and then click **Next**.

3. On the **Server Role** page, in the list under **Server Role**, click **Domain Controller (Active Directory)**, as illustrated in the following figure.



This automatically launches the Active Directory Installation Wizard.

4. On the Welcome page, click **Next**.
5. On the Domain Controller Type page, shown in the following figure, click **Domain controller for a new domain**, and then click **Next**.



6. On the **Create New Domain** page, click **Domain in a new forest**, and then click **Next**.

The Wi-Fi Authentication Test Suite must be run against a private network, one that is isolated from the corporate network. For this reason, this domain controller must be a root domain controller.

7. On the **New Domain Name** page, enter the name of the new domain, and then click **Next**.

 **Important:**

Use the .local label, for example, Wince.local, because this provides a more secure configuration for your test environment than using other labels. It is not registered for use on the Internet and will prevent the server from attempting to authenticate itself against a higher domain.

8. On the **Database and Log Folders** page, keep the default values for the **Database folder** and **Log Folder**, and then click **Next**.

 **Important:**

If you want to change the location of these folders, you can do so, but the drive that you use must be a local resource and it must not be mapped to a network path.

9. On the **Shared System Volume** page, keep the default value for **Folder location**, and click **Next**.

For the Wi-Fi Authenticate Test Suite, setting a shared system volume is irrelevant.

The process for setting up DNS server functionality begins with the next page of the Active Directory Installation Wizard. See [How To Set Up a DNS Server](#).

See Also

Other Resources

[How To Set Up the Windows Mobile Authentication Servers on Windows Server 2003](#)

[Wi-Fi Authentication Tests](#)

How To Set Up a DNS Server

8/27/2008

Before you set up a DNS server, you must install Active Directory as described in [How To Set Up Active Directory](#). To ensure that the DNS server is properly installed and configured for successful Wi-Fi testing, set it up as part of your Active Directory installation. The following figure shows the Active Directory Installation Wizard message you will see at the end of Active Directory installation and prior to DNS server configuration.



To set up a DNS server

1. In the Active Directory Installation Wizard, on the **DNS Registration Diagnostics** page, select **Install and configure the DNS server on this computer, and set this computer to sue this DNS server as its preferred DNS server**, and then click **Next**.
2. On the **Permissions** page, click **Permissions compatible only with the Windows 2000 Server or Windows Server 2003 operating systems.**, and then click **Next**.
3. On the **Directory Services Restore Mode Administrator Password** page, set the **Restore Mode Password** and confirm it.

In your test environment, using this restore-mode password is not likely to be necessary. For the purpose of setting up the test environment, however, set this password to be the same as the Administrator account that you created when you installed Windows Server 2003.

Click **Next**.

4. On the **Summary** page, review the choices that you have made for setting up and configuring Active Directory and the DNS service for your server.
5. Click **Next** to start the launch the setup process.

The process takes between ten and fifteen minutes, depending on the speed of the computer being used. While the process is running, it will periodically display status screens that indicate the actions being taken.

 **Important:**

Make sure that you have the Windows Server 2003 installation disk available, because the system may require it at this point to complete the setup process.

- When the **Optional Networking Components** message appears, click **OK**.
- In the **Internet Protocol (TCP/IP) Properties** dialog box, click **Use the following IP address**, and assign a static IP address to the server.

The static IP address can be any private-range IP address. Because Wi-Fi testing requires frequent use of this IP address, assign one that is easy to remember, for example, **10.10.0.1**.

- Click **Next**.

The Active Directory Installation Wizard configures the DNS service on the computer. This process should only take a few minutes.

⚠ Caution:

Make sure that you allow this configuration process run to completion. In the configuration status message that appears, do not click **Skip DNS Installation**. If you skip the installation, your test environment will not work with the Wi-Fi Authentication Test Suite.

- When the DNS installation is complete, the **Completing the Active Directory Installation Wizard** page opens. Click **Finish**.
- Restart your computer by clicking **Restart now** in the notification message that appears.
- When the computer restarts, the following confirmation page opens.



- Click **Finish**.

See Also

Other Resources

[How To Set Up the Windows Mobile Authentication Servers on Windows Server 2003](#)

[Wi-Fi Authentication Tests](#)

How To Set Up a DHCP Server



8/27/2008

After you have installed Windows Server 2003 and configured it for Active Directory and DNS, you are ready to set up the DHCP server for your test environment.

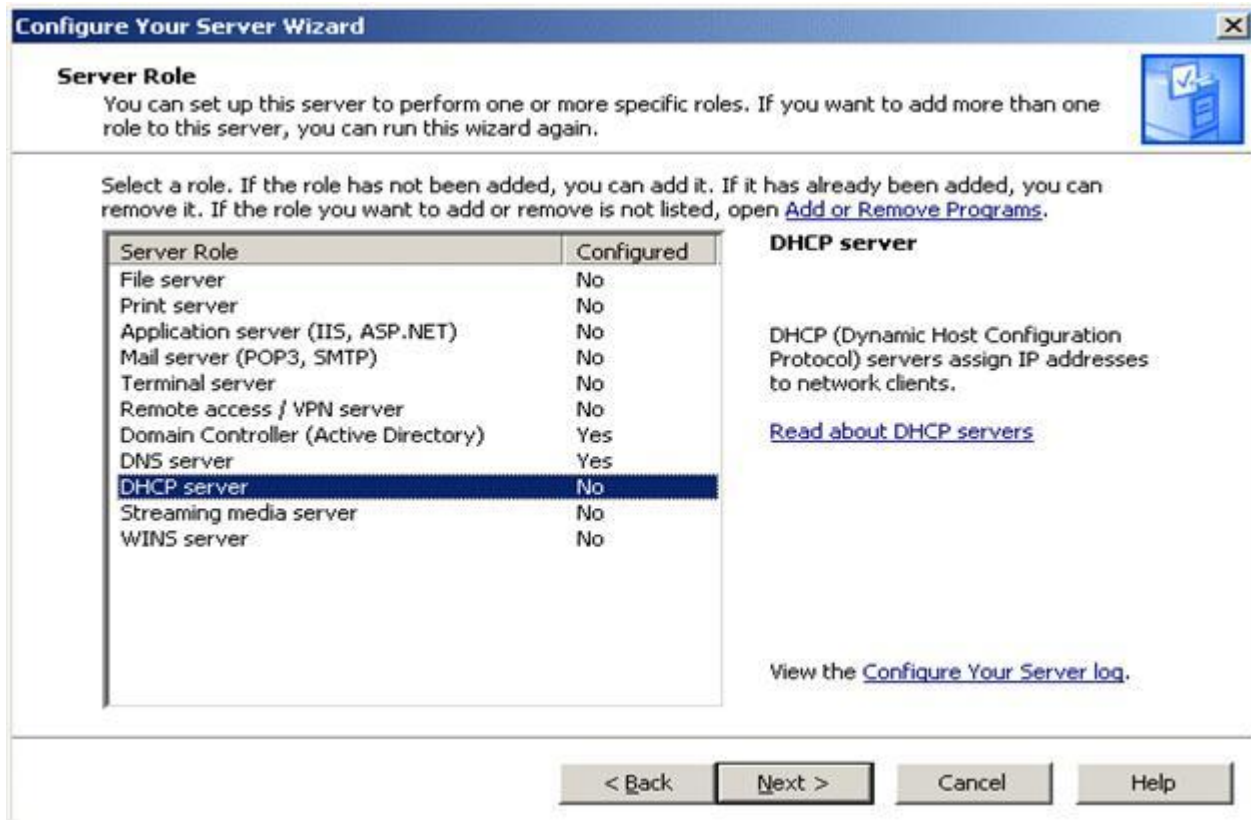
Note:

If the private network that you have established for testing already includes a previously configured DHCP server, you may skip this section.

Procedure

To set up your DHCP server

1. In the **Manage Your Server** window, click **Add or remove a role**.
2. In the Configure Your Server Wizard, on the **Server Role** page, select **DHCP Server** from the list, as shown in the following figure, and then click **Next**.



This adds the new role to your server.

3. On the **Summary of Selections** page, review the server options that you have chosen, and then click **Next**.
The **New Scope Wizard** opens.
4. On the **Welcome** page, click **Next**.
5. On the **Scope Name** page, enter a name and a description for the scope of the server.

Note:

The name that you provide here does not affect the configuration or how IP address requests are served.

- Click **Next**.
- On the **IP Address Range** page, provide a range of IP addresses for this server to assign. See the example in the following figure.

New Scope Wizard

IP Address Range
You define the scope address range by identifying a set of consecutive IP addresses.

Enter the range of addresses that the scope distributes.

Start IP address: 10 . 10 . 0 . 100

End IP address: 10 . 10 . 0 . 200

A subnet mask defines how many bits of an IP address to use for the network/subnet IDs and how many bits to use for the host ID. You can specify the subnet mask by length or as an IP address.

Length: 24

Subnet mask: 255 . 255 . 255 . 0

< Back Next > Cancel

This is range of addresses is the scope of your DHCP server. For best results, provide a range of at least 10 IP addresses and no more than 245 addresses.

- Click **Next**.
- On the **Add Exclusions** page, if the DHCP scope you entered in step 7 includes all of the IP addresses on your subnet, you must reserve static IP addresses for the AP control server and the RADIUS server here. However, if the scope does not contain all of the IP addresses of the subnet that you created, you can ignore this page.

Note:

"Exclusions" are either individual IP addresses or a range of IP addresses that are not distributed by the DHCP server.

- Click **Next**.
- On the **Lease Duration** page, accept the default setting of eight days by clicking **Next**.
The lease duration is the length of time a client device may use an assigned IP address.
- On the **Configure DHCP Options** page, click **Yes, I want to configure these options now**, and then click **Next**.
This ensures that the DHCP clients in your test environment can use the assigned scope.
- On the **Router (Default Gateway)** page, leave all of the fields blank, and click **Next**.
These fields are not used for this test environment.
- On the **Domain Name and DNS Servers** page, enter the name of the parent domain, and the name of the server, and the IP address that you specified during the process of installing Active Directory.

Note:

If you cannot remember the names or IP address that you assigned to the server, you can find them by going to Control Panel and clicking **System Properties**, and then clicking the **Computer Name** tab.

15. Click **Next**.

16. If you plan to use WINS, on the **WINS Servers** page, specify the WINS server name and IP address.

Note:

The test environment for Windows Mobile and the Wi-Fi Authentication Test Suite does not require the use of WINS.

17. On the **Activate Scope** page, click **Yes, I want to activate this scope now**, and then click **Next**.

This activates the scope.

18. When the wizard is done, click **Finish**.

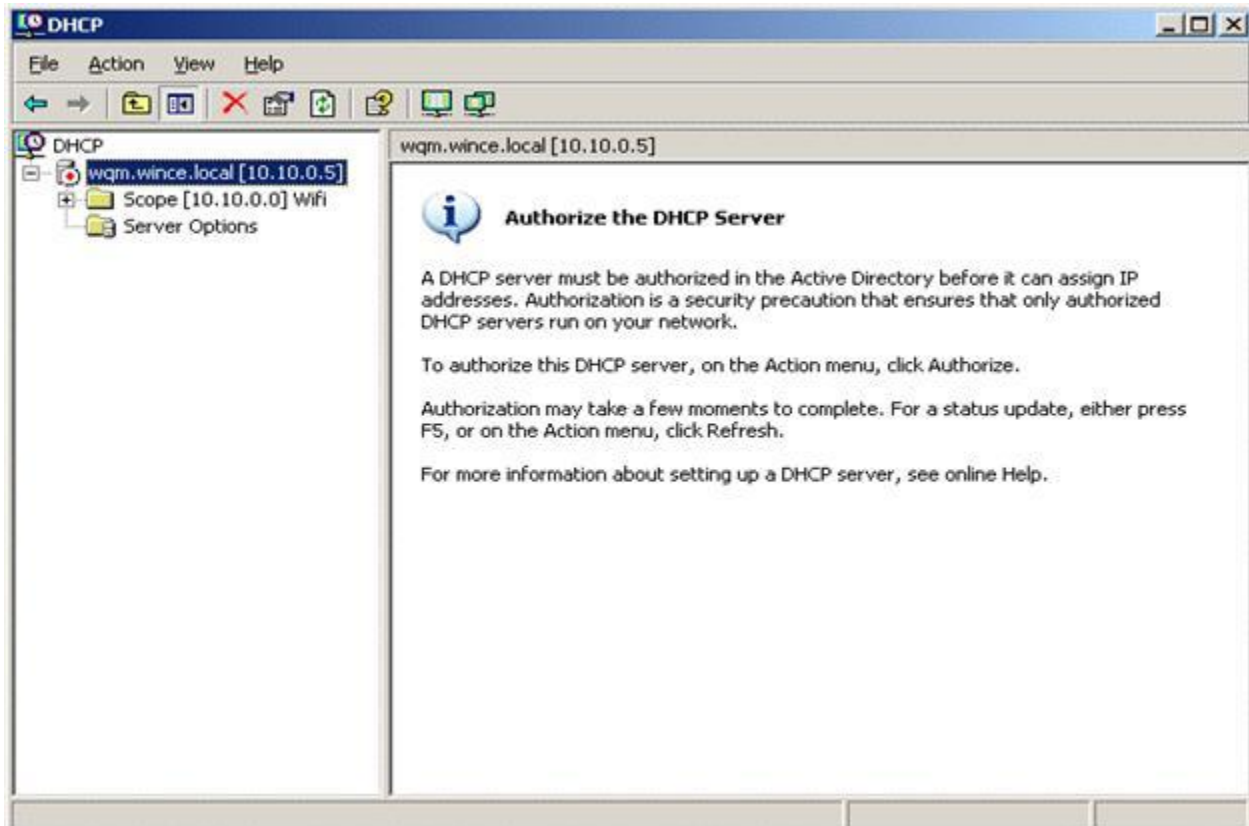
If this is the first time you have worked through the Configure Your Server Wizard, a confirmation screen appears, explaining the changes that have been made.

Important:

Before the server can process DHCP requests, you must authorize the scope in Active directory, as described in the next procedure.

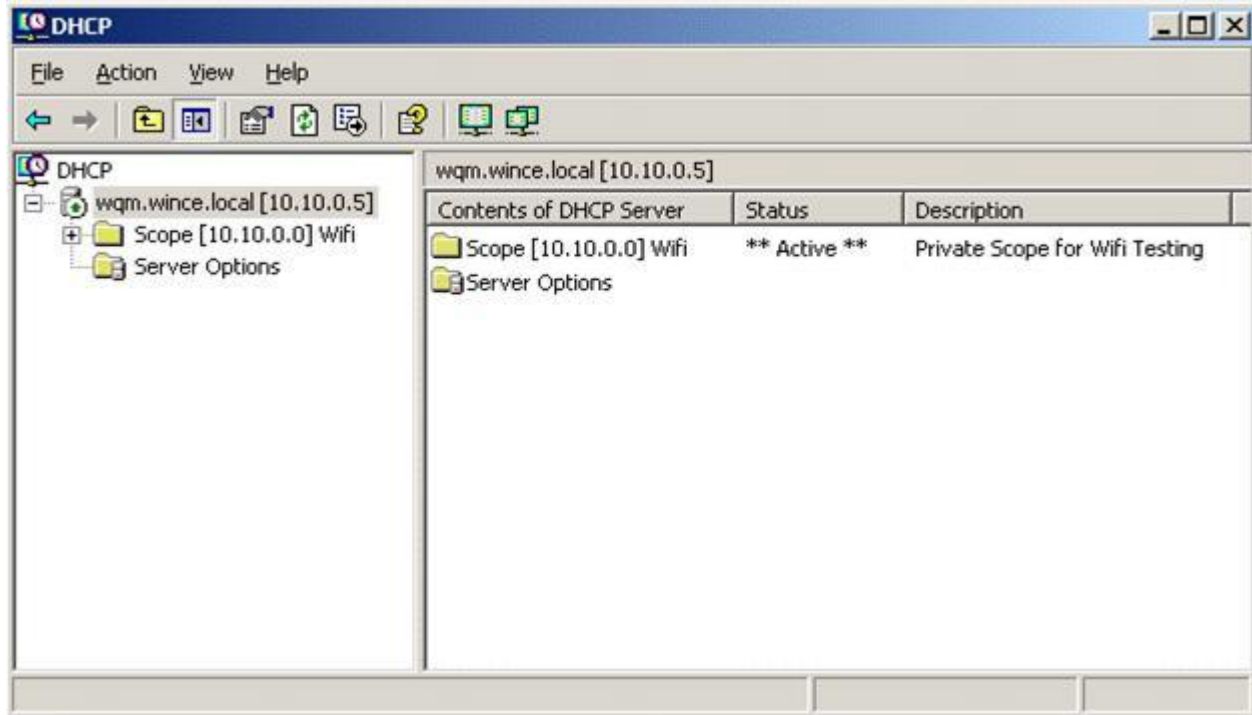
To authorize the DHCP server scope in Active Directory

1. On the **Start** menu, click **Administrative Tools**.
2. Open the **DHCP Management Console**.
3. In the pane on the left, under **DHCP**, select the fully-qualified domain name of the test server that you have just configured, as shown in the following figure.



4. To authorize the DHCP server, in the Toolbar, click the **Authorization** icon .

When the authorization process is complete, the right pane of the DHCP console window shows that the scope is active, as illustrated in the following figure.



 **Note:**

If the status of the **Scope** node in the right pane does not indicate that it is active after a few minutes, press F5 to refresh the screen.

See Also

Tasks

[How To Set Up Active Directory](#)

[How To Set Up a DNS Server](#)

Other Resources

[How To Set Up the Windows Mobile Authentication Servers on Windows Server 2003](#)

[Wi-Fi Authentication Tests](#)

How To Set Up Internet Information Services



8/27/2008

After you have installed Windows Server 2003, installed and configured Active Directory, and set up the DNS server and DHCP server, you must add the Application Server role that contains Internet Information Services (IIS). IIS is required so that the authentication server is able to provide certificates to client devices.

To install Internet Information Services

1. In the **Manage Your Server** window, click **Add or remove a role**.
2. In the Configure Your Server Wizard, on the **Server Role** page select **Application Server (IIS, ASP.NET)** from the list, and then click **Next**.
3. On the **Application Server Options** page, select the **Enable ASP.NET** check box, and then click **Next**.

4. On the **Summary of Selections** page, review and confirm the options that are included with IIS and ASP.NET, and then click **Next**.

The installation of these service components on the server starts. Installing and configuring Internet Information Services and its related components only takes a few minutes.

5. When the installation is complete and the confirmation page displays, click **Finish** to close the wizard.

See Also

Other Resources

[How To Set Up the Windows Mobile Authentication Servers on Windows Server 2003](#)

[Wi-Fi Authentication Tests](#)

How To Set Up the Internet Authentication Service



8/27/2008

After you have installed Windows Server 2003, have installed and configured Active Directory, have set up the DNS and DHCP servers, and have set up IIS, you must install and configure the Internet Authentication Service (IAS) so that your test environment functions properly when you are running the Wi-Fi Authorization Test Suite.

Procedure

Set up the Internet Authentication Service

1. On the **Start** menu, click **Control Panel**.
2. Double-click **Add or Remove Programs**.
3. Click **Add/Remove Windows Components**.
4. In the Windows Components Wizard, on the **Windows Components** page, do the following:
 - a. Select the **Networking Services** check box.
 - b. Click **Details** to see a list of the available Networking Services.
5. On the **Networking Services** page:
 - a. Make sure that both the **Domain Name System (DNS)** check box and the **Dynamic Host Configuration Protocol (DHCP)** check box are selected.
 - b. Select the **Internet Authentication Service** check box, and select the **Simple TCP/IP Services** check box.

Note:

The Echo service component, which is required, is automatically installed when you install the Simple TCP/IP services.

6. Click **OK** to begin installation of the added networking services.

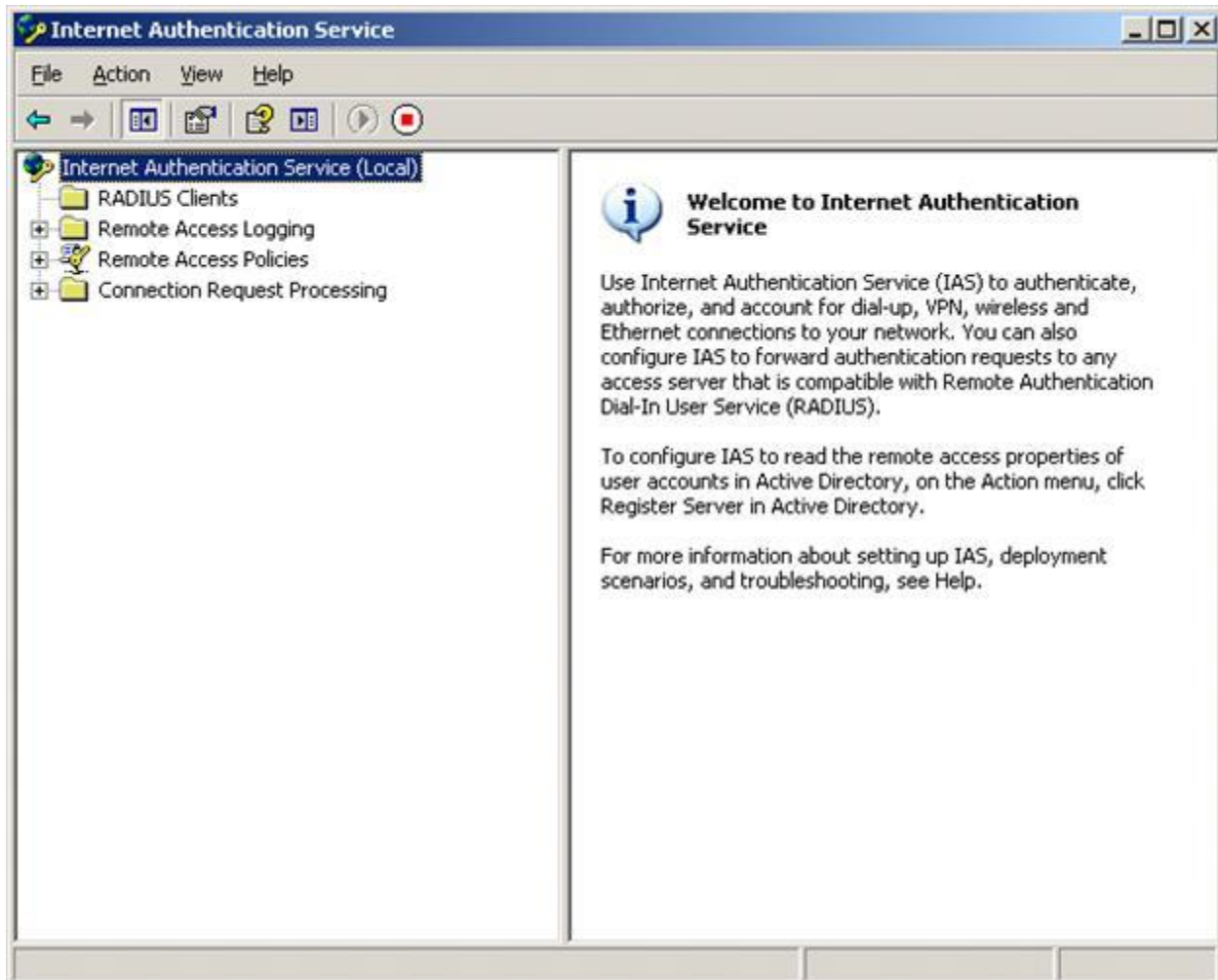
When the installation is finished, the Windows Components Wizard indicates that the installation was successful.

7. Click **Finish**.

Now you must register the Internet Authorization Service in Active Directory.

Register the Internet Authentication Service

1. On the **Start** menu, click **Administrative Tools**.
2. In **Administrative Tools**, open the Internet Authentication Service management console.
3. In the Internet Authentication Service management console, in the left pane of the window, select **Internet Authentication Service (Local)**, as illustrated in the following figure.



4. On the menu bar, click **Action**.
5. On the **Action** menu, click **Register Server in Active Directory**.
6. In the **Register Internet Authentication Server in Active Directory** message that opens, click **OK**.

See Also

Other Resources

[How To Set Up the Windows Mobile Authentication Servers on Windows Server 2003](#)

[Wi-Fi Authentication Tests](#)

How To Set Up the AP Control Server



8/27/2008

The AP control server handles access point configuration requests from the test device and updates the access point with the necessary authentication and encryption methods. For more information, see [Wi-Fi Authentication Tests Overview](#) topic,

For your test environment, the AP control server is the server on which you installed the Internet Authentication Service.

Procedure

To configure the AP control server

1. Enter the registry settings for each access point that the server is to control. Each entry must contain the following settings shown in the following table.

SSID

This is the service set identifier that serves as the unique name of the access point

Attenuator

This is the setting that is required by the AP control server, even though the setting is not used for the Wi-Fi Authentication Test itself.

The syntax for this setting is:

For test purposes, always set this value to **Manual;0.0.100**.

Configurator

This is the setting that tells the server how to contact the access point. The syntax for this setting is:

```
{deviceType};{nameAddress}[:{adminUser}:{adminPassword}]
```

- Set the deviceType value to **dlink**, **buffalo**, or **manual**.
- Set the nameAddress value to the IP address of the access point.
- Do not include a value for adminUser unless it has been changed from the factory default.
- Do not include a value for adminPassword unless it has been changed from the factory default.

For more information, see [Access Point Registry Settings for the Wi-Fi Authentication Tests](#).

For a list of access points that are supported by the AP control server, see [Supported Access Points for the Wi-Fi Authentication Tests](#)

2. From a command prompt, enter the command to tell the server which port it should use for accepting connections and where the server will find the initial configuration information for the access point it controls. For more information, see [Command-Line Parameters for use with the AP Control Server](#)

See Also

Concepts

[Example Test Configurations for the Wi-Fi Configuration Tests](#)

Other Resources

[How To Set Up the Windows Mobile Authentication Servers on Windows Server 2003](#)

[Wi-Fi Authentication Tests](#)

Supported Access Points for the Wi-Fi Authentication Tests



8/27/2008

The following table shows the access points that are supported by the AP control server.

| Vendor and model | Firmware | Supported modes |
|------------------------------|--|---|
| Buffalo AirStation WBR2-G54S | Version 2.30 or higher | Open Shared WPA WPA-AES WPA-PSK |
| Buffalo AirStation WBR2-G54S | Broadcom: <ul style="list-style-type: none"> • CFE 3.52.21.10 • Linux 3.131.20.0 | Open Shared WEP-802.1X WPA WPA-AES WPA-PSK WPA2 WPA2-PSK |

| | | |
|------------------|----------------------|---|
| Cisco AIR-1232AG | 12.3(8)JEA1 | Open Shared WEP-802.1X WPA WPA-TKIP WPA2 WPA2-AES |
| D-Link DWL-3200 | Version 2.10 or 2.20 | Open Shared WPA WPA-AES WPA-PSK WPA2 WPA2-PSK |

See Also

Tasks

[How To Set Up the AP Control Server](#)

Other Resources

[How To Set Up the Windows Mobile Authentication Servers on Windows Server 2003](#)

[Wi-Fi Authentication Tests](#)

Access Point Registry Settings for the Wi-Fi Authentication Tests



8/27/2008

The following example shows a registry file that describes two access points.

[Copy Code](#)

```
[HKEY_CURRENT_USER\Software\Microsoft\CETest\APCTL\AP1]
"CapsImplemented"="WPA,WPA_PSK,WPA2,WPA2_PSK"
"CapsEnabled"="WPA,WPA_PSK,WPA2,WPA2_PSK"
"RadioState"=dword:00000001
"SSID"="WIFI_OPEN_1"
"BSSID"=hex:00,13,46,89,b9,db
"Authentication"="WPA2_PSK"
"Cipher"="TKIP"
"RadiusServer"="10.10.0.1"
"RadiusPort"=dword:00001812
"RadiusSecret"="0123456789"
"WEPIndex"=dword:00000000
"WEPKey0"=hex:a0,b0,c0,d0,e0
"WEPKey1"=hex:f1,a2,b3,c4,d5
"WEPKey2"=hex:e2,f3,a4,b5,c6
"WEPKey3"=hex:d3,e4,f5,a6,b7
"Passphrase"="0123456789"
"Configurator"="dlink;10.10.0.48"
"Attenuator"="Manual;0,0,100"

[HKEY_CURRENT_USER\Software\Microsoft\CETest\APCTL\AP2]
"CapsImplemented"="WEP_802_1X,WPA,WPA_PSK,WPA2,WPA2_PSK"
```

```
"CapsEnabled"="WEP_802_1X,WPA,WPA_PSK,WPA2,WPA2_PSK"
"RadioState"=dword:00000001
"SSID"=" WIFI_OPEN_2"
"BSSID"=hex:00,13,46,89,b9,db
"Authentication"="WPA2_PSK"
"Cipher"="TKIP"
"RadiusServer"="10.10.0.1"
"RadiusPort"=dword:00001812
"RadiusSecret"="0123456789"
"WEPIndex"=dword:00000000
"WEPKey0"=hex:a0,b0,c0,d0,e0
"WEPKey1"=hex:f1,a2,b3,c4,d5
"WEPKey2"=hex:e2,f3,a4,b5,c6
"WEPKey3"=hex:d3,e4,f5,a6,b7
"Passphrase"="0123456789"
"Configurator"="buffalo;10.10.0.16:admin:password"
"Attenuator"="Manual;0,0,100"
```

In the first example, the access point is named AP1, as indicated in the first line of the registry key setting. The SSID is WIFI_OPEN_1. Looking at the Configurator entry, you can see that this D-Link access point can be contacted at IP address 10.10.0.48 with the default administrator name and password.

In the second example, the access point is named AP2. The SSID is WIFI_OPEN_2. Again, looking at the Configurator entry, you can see that this access point is a Buffalo AP, and its IP address is 10.10.0.16. Note, however, that unlike the D-Link AP, you must use the administrator name **admin** and provide **password** as the password to contact this access point.

As noted in the topic [How To Set Up the AP Control Server](#), the only required registry setting values are SSID, Configurator, and Attenuator. The other settings are optional and, if supplied by the user, are ignored. The reason these values appear in these examples is that the server automatically retrieves them from the controlled access points, and all retrieved values are displayed in the registry editor.

See Also

Concepts

[Supported Access Points for the Wi-Fi Authentication Tests](#)

Other Resources

[How To Set Up the Windows Mobile Authentication Servers on Windows Server 2003](#)

[Wi-Fi Authentication Tests](#)

Command-Line Parameters for use with the AP Control Server



8/27/2008

The AP control server is the server on which you have installed Internet Authentication Services (IAS). Launch this service, and start the AP control server from the command-line.

For more information, see [How To Set Up the AP Control Server](#),

Syntax


```
apcontrol.exe [ -s server ] [ -p port ] [ -v ] [ -z ] [ -k regKey ]
```

Command-line parameters

| Command-line | Description |
|--------------|-------------|
|--------------|-------------|

Writing Sample--Windows Mobile Wireless Tests—"After" Example
Katy Koenen

| parameter | |
|-------------------------|--|
| -s <i>server</i> | Specifies the name or the IP address of the server. The default value is localhost , |
| -p <i>port</i> | Specifies the TCP/IP port through which the AP control server connects to the access points. The default value is 33331 . |
| -v | Specifies that debug output be verbose. |
| -z | Sends debug output to the console. |
| -k <i>regKey</i> | Specifies the registry key that contains the initial configuration for the access point. The default value is SOFTWARE\Microsoft\CETest\APCTL . |
| -? | Provides information about the command-line parameter. |

 **Note:**

Normally, only the port and the registry key are specified.

See Also

Concepts

[Supported Access Points for the Wi-Fi Authentication Tests](#)

Other Resources

[How To Set Up the Windows Mobile Authentication Servers on Windows Server 2003](#)

[Wi-Fi Authentication Tests](#)

How To Set Up RADIUS Clients



8/27/2008

In the context of the Wi-Fi test network, the RADIUS clients are the access points that are attached to the test network.

Procedure

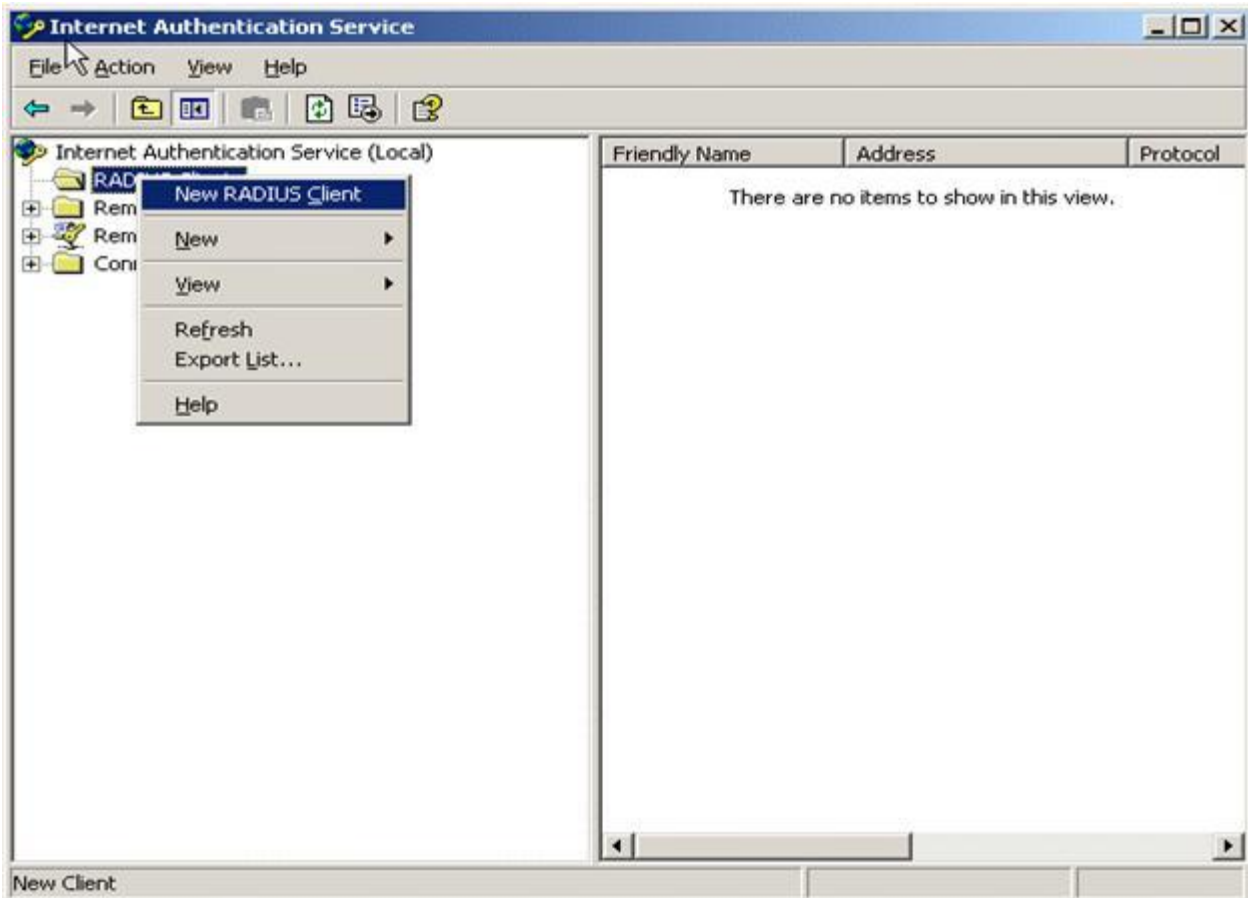
To set up RADIUS clients

1. On the **Start** menu, click **Administrative Tools**.
2. Open the **Internet Authentication Service (IAS)** console.

 **Note:**

The IAS console does not appear as an option in **Administrative Tools** until you have installed IAS.

3. In the left pane of the window, right-click **RADIUS client**, and then click **New**.



4. In the New Radius Client wizard, on the **Name and Address** page, enter a friendly name and an IP address for the access point, and then click **Next**.

Caution:

The IP addresses must be from the same subnet as the scope that was set up in the DHCP server.

5. On the **Additional Information** page, in the **Client-Vendor** box, keep the default value **RADIUS Standard**.
6. In the **Shared secret** box, enter a shared key, and then **confirm** it.

Note:

The same key must be configured on the access point to ensure that the server can communicate certificate information to and from the access point.

7. Click **Finish**.

See Also

Other Resources

[How To Set Up the Windows Mobile Authentication Servers on Windows Server 2003](#)

[Wi-Fi Authentication Tests](#)

How To Set Up Certificate Services



8/27/2008

Procedure

To install Certificate Services

1. On the **Start** menu, click **Control Panel**.

Writing Sample--Windows Mobile Wireless Tests—"After" Example
Katy Koenen

2. In Control Panel, double-click **Add or Remove Programs**.
3. Click **Add/Remove Windows Components**.
4. In the Windows Components Wizard, on the **Windows Components** page, in the list under **Components**, select **Certificate Services**, and then click **Details**.
5. On the **Certificate Services** page, select both **Certificate Services CA** and **Certificate Services Web Enrollment Support**.
Click **OK**.
6. When the warning message opens, click **Yes**.

Important:

After you click **Yes**, you may not change the name of any of the computers or domains on the network. Later, if you need to change any of these names, you must reinstall all the server software and roles.

1. A second warning message explains that the Internet Information Services must be stopped before the installation of Certificate Services can be completed.
Click **Yes**.
2. On the **CA Type** page, click **Enterprise root CA**, and then click **Next**.
3. On the **CA Identifying Information** page, in the **Common name for this CA** box, enter the root name for the domain on which the server is installed.
Click **Next**.
4. On the **Certificate Database Settings** page, accept the default certificate log locations by clicking **Next**.
5. The last page of the wizard indicates whether the installation was successful.
6. Click **Finish**.

See Also

Other Resources

[How To Set Up the Windows Mobile Authentication Servers on Windows Server 2003](#)

[Wi-Fi Authentication Tests](#)

How To Enable Certificate Templates



8/27/2008

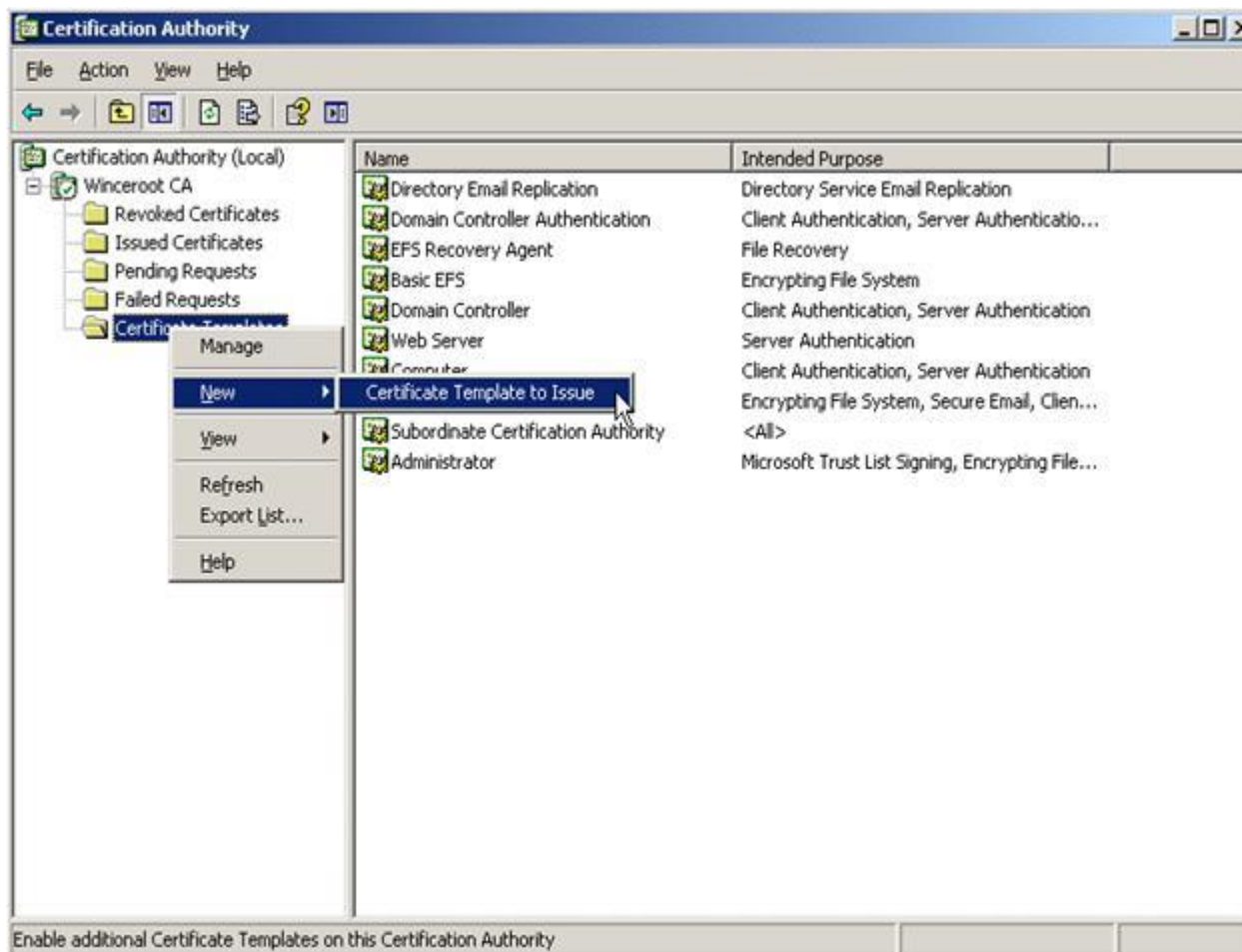
To enable certificate templates, you must first allow Enroll permissions for authenticated users.

To enable Enroll Permissions for authenticated users on Certificate Templates

1. On the **Start** menu, click **Run**.
2. In the **Run** dialog box, type **certtmpl.msc**, and then click **OK** to install the Certificate Template.
3. In the Certificate Templates Management console, right-click the **Computer** template.
4. In the **Computer Properties** dialog box, click the **Security** tab, and then under **Group or user names**, click **Authenticated Users**,
5. Under **Permissions for Authenticated Users**, select the **Allow** check box for each type of permission that you want assign to this group, and then click **OK**.
6. Close the **Computer** template.
7. Close the **Certificate Templates Management** console.

To install Certificate Templates into Certificate Services

1. On the **Start** menu, click **Run**.
2. In the **Run** dialog box, type **certtmpl.msc**, and then click **OK** to install the certificate template.
3. On the **Start** menu, click **Administrative Tools**.
4. In **Administrative Tools**, click **Certification Authority Console**.
5. In the left pane of the Certification Authority window, right-click **Certificate Template**, click **New**, and then click **Certificate Template to Issue**.



6. In the **Enable Certificate Templates** dialog box, select all entries in the list by doing the following:
 - a. Select the first entry in the list
 - b. Press the SHIFT key while clicking the left mouse button
 - c. Click the last entry in the list
7. Click **OK**.

See Also

Other Resources

[How To Set Up the Windows Mobile Authentication Servers on Windows Server 2003](#)

[Wi-Fi Authentication Tests](#)

How To Create User Groups and Remote Accounts



8/27/2008

Writing Sample--Windows Mobile Wireless Tests—"After" Example
Katy Koenen

To run the Wi-Fi Authentication Test, you must create the following user groups and accounts shown in the following table.

| User groups | User accounts |
|----------------|---------------------------------------|
| EAP-TLS Users | Username: eaptls / Password: eaptls |
| EAP-PEAP Users | Username: eappeap / Password: eappeap |
| EAP-MD5 Users | Username: eapmd5 / Password: eapmd5 |

 **Note:**

You must follow all three procedures that are described here for each user account and each user group in the preceding table.

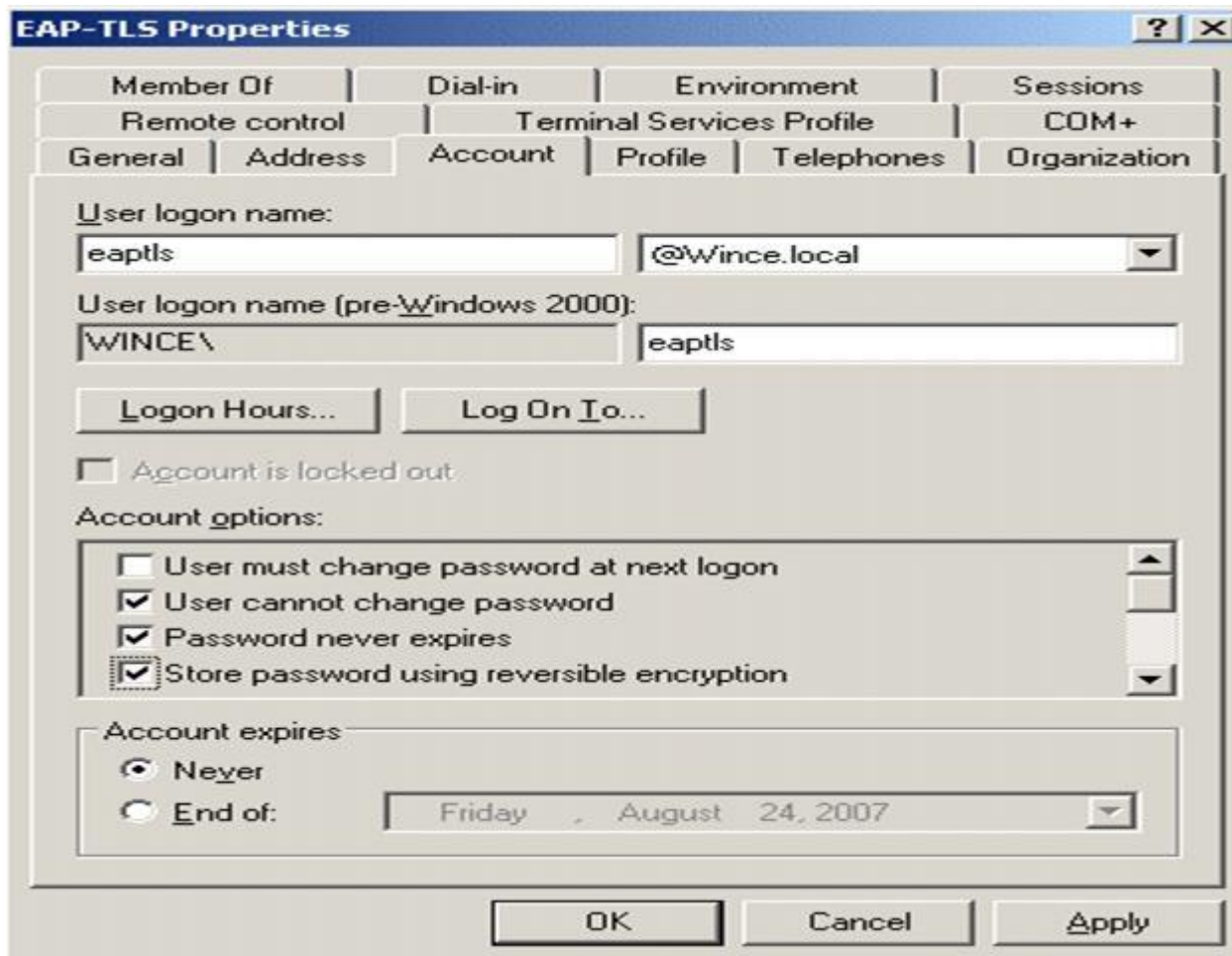
Procedure

To set up user groups

1. On the **Start** menu, right-click **My Computer**, and then click **Manage**.
2. In the console tree in the left pane, click **System Tools**, then **Local Users and Groups**, and then double-click **Groups**.
3. Click **Action**, and then click **New Group**.
4. In the **Group name** box, type a name for the new group.
5. In the **Group Scope** list, select **Global**.
6. In the **Group Type** list, select **Security**.
7. Click **OK**.

To set up user accounts

1. On the **Start** menu, right-click **My Computer**, and then click **Manage**.
2. In the console tree in the left pane, click **System Tools**, click **Local Users and Groups**, and then double-click **Users**.
3. Click **Action**, and then click **New User**.
4. In **User name** box, type the name for the new user account, and then click **Next** to launch the New Object - User wizard.
5. In the first dialog box, enter and confirm the password for the user account in the appropriate boxes.
6. Select the **User cannot change password** check box, and then select the **Password never expires** check box.
7. Click **Next**.
8. Right-click **Properties**, and then click the **Account** tab.
9. Select the **Store password using reversible encryption** check box.



10. Click the **Dial-in** tab.

11. Under **Remote Access Permission (Dial-in or VPN)**, select **Allow access**, and then click **OK**.

To add user accounts to user groups

1. On the **Start** menu, right-click **My Computer**, and then click **Manage**.
2. In the console tree in the left pane, click **System Tools**, click **Local Users and Groups**, and then double-click **Groups**.
3. Right-click the newly created group to open the **Select Users, Contacts or Computers** dialog box.
4. In the **Enter the object names to select** box, enter the user account name for the appropriate group, and then click **OK**.

See Also

Other Resources

[How To Set Up the Windows Mobile Authentication Servers on Windows Server 2003](#)

[Wi-Fi Authentication Tests](#)

How To Create Remote Policies by Using IAS



8/27/2008

To ensure that the Wi-Fi Authorization Test runs properly, you must repeat the following procedure for each user group that you have created.

Procedure

To set up remote policies by using the Internet Authorization Service

1. On the **Start** menu, click **Administrative Tools**.

Writing Sample--Windows Mobile Wireless Tests—"After" Example
Katy Koenen

2. In **Administrative Tools**, click **Internet Authentication Service Management** console.
3. In the **Internet Authentication Service** management console, click **Action**.
4. On the **Action** menu, click **New Remote Access Policy**, and then click **Wireless**.
Click **Next**.
5. In the **New Remote Access Policy** Wizard, on the **User or Group Access** page, click **Group**, and then click **Add**.
6. In the **Select Groups** dialog box, under **Enter the object names to select**, enter the appropriate user group for this policy, and click **OK**, and then click **Next**.
7. On the **Authentication Methods** page, under **Type**, select either **Smart Card or other certificate** or **Protected EAP (PEAP)** from the list, and then click **Next**.
8. When the system finishes applying the policy, on the last page of the wizard, click **Finish**.

 **Note:**

This procedure applies the designated policy to the user group, not to individual users.

See Also

Other Resources

[How To Set Up the Windows Mobile Authentication Servers on Windows Server 2003](#)

[Wi-Fi Authentication Tests](#)

Verifying the Test Environment for Wi-Fi Authentication Tests



8/27/2008

Before you run any of the Wi-Fi Authentication Tests, you must verify that the complete RADIUS server test environment is properly established.

To validate the test environment

1. Reboot your server.
2. After your system is back online, make sure the computer that hosts the AP control server and RADIUS server has static IP addresses.
3. Make sure that the device that is being tested can connect to the fixed access point
4. Verify that an IP address is dynamically assigned to the device.

See Also

Tasks

[Establishing the Correct Test Environment for Wi-Fi Authentication Tests](#)

Other Resources

[How To Set Up the Windows Mobile Authentication Servers on Windows Server 2003](#)

[Wi-Fi Authentication Tests](#)

How To Configure Wi-Fi Authentication Access Points



8/27/2008

To run any of the Wi-Fi Authentication tests, you must configure the access points (APs) so that one is *fixed*, meaning that its configuration does not change and the AP Control server does not manage it. This AP acts as the static association point for devices connecting to the AP Control server.

Writing Sample--Windows Mobile Wireless Tests—"After" Example
Katy Koenen

You must also configure one or more other access points that the AP Control server manages.

To set up a fixed access point

1. Set the SSID for the fixed access point to `WIFI_OPEN..`

 **Important:**

The authentication mode for the fixed access point must not require 802.1x (EAP) authentication, because at the beginning of the test, the device does not have all the certificates required to authenticate itself to the RADIUS server.

2. Give the access point a static IP address.

For a list of access points that are supported by the AP control server, see [Supported Access Points for the Wi-Fi Authentication Tests](#)

To set up a controllable access point

1. Manually configure each controllable access point so it communicates properly with the RADIUS server:
 - a. Specify the server's IP address.
 - b. Specify the port through which the access points will communicate with the server, typically 1812.
 - c. Specify the shared key.
2. Configure each access point with a static IP address.
3. Connect to each of the access points from the AP Control server. To test each connection, retrieve the following initial information from each of the access points on the network:
 - SSID
 - IP Address
 - Administrator user name and password

For more information, see [How To Set Up RADIUS Clients](#).

See Also

Other Resources

[How To Set Up the Windows Mobile Authentication Servers on Windows Server 2003](#)

[Wi-Fi Authentication Tests](#)

Running the Wi-Fi Authentication Tests



8/27/2008

The Wi-Fi Authentication Tests are implemented as a Tux DLL, named AuthMatrix.dll, and these tests comprise multiple test cases for seven different types of Wi-Fi authentication. For more information on the specific test cases, see [Test Cases for the Wi-Fi Authentication Test](#).

Procedure

To run the Wi-Fi Authentication Tests

1. Verify that the test environment is set up correctly. For more information on setting-up the proper test environment, see [Establishing the Correct Test Environment for Wi-Fi Authentication Tests](#). For more information on validating the test environment, see [Verifying the Test Environment for Wi-Fi Authentication Tests](#).
2. At a command prompt on the AP Control server, start the AP Control server.
3. At the command prompt on the device, enter the Tux command with the options required for the test you want to run.

For information on the Tux command-line options, see [Tux Command-Line Parameters](#).

See Also

Tasks

[Establishing the Correct Test Environment for Wi-Fi Authentication Tests](#)

Reference

[Command Line Parameters for the Wi-Fi Authentication Tests](#)

Concepts

[Example Test Configurations for the Wi-Fi Configuration Tests](#)

Other Resources

[Wi-Fi Authentication Tests](#)

Example Test Configurations for the Wi-Fi Configuration Tests



8/27/2008

The following examples illustrate ways to run the Wi-Fi Authentication Tests with different components and configurations.

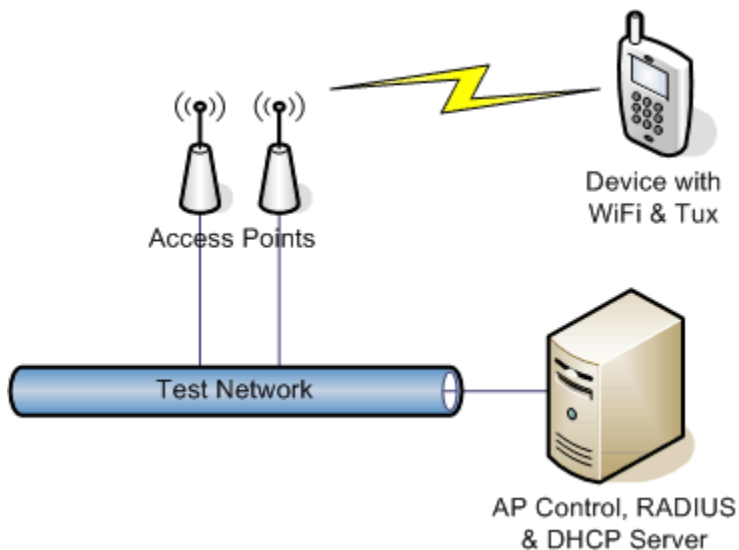
[Single Server and Access Point](#)

[Separate Servers and Multiple Access Points](#)

Single Server and Access Point

This environment has only one server and one controllable access point (AP). The following illustration shows this architecture:

- A fixed access point
- A controllable access point
- A single computer with an IP address of 10.10.0.1, which acts as the AP Control server, the RADIUS server, and the DHCP server
- A test network
- A mobile device



The fixed access point has the following configuration:

- SSID: WIFI_OPEN
- Authentication: Open
- Encryption: WEP
- WEP-Key Index: 1
- WEP key: 0123456789

The following registry key and registry values control the behavior of the controllable access point:

HKEY_CURRENT_USER\Software\Microsoft\CETest\APCTL\AP1

| Value | Type | Description |
|--------------|--------|-------------------|
| SSID | REG_SZ | WIFI_OPEN1 |
| Configurator | REG_SZ | dlink; 10.10.0.48 |
| Attenuator | REG_SZ | Manual; 0,0,100 |

At a command prompt on the server, run the following command:

```
apcontrol.exe -v -z -k Software\Microsoft\CETest\APCTL
```

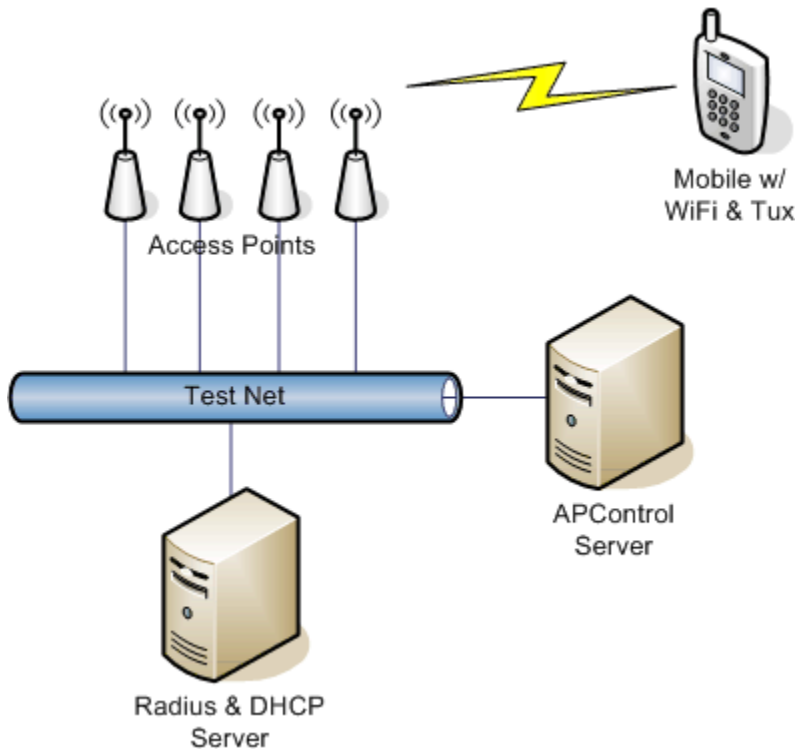
At a command prompt on the device, run the following command:

```
\Windows\tux.exe -f\temp\amdebug.log -d authmatrix.dll  
-c "-lHost 10.10.0.1"
```

Separate Servers and Multiple Access Points

This environment has servers that run on separate computers, and three controllable APs. The following illustration shows this architecture:

- A fixed access point
- Three controllable access points
- An AP Control server at IP address 10.10.0.2
- A combined RADIUS and DHCP server at IP address 10.10.0.1
- A test network
- A mobile device



In this example, the fixed access point is configured as follows:

- SSID: WIFI_OPEN

- Authentication: WPA-PSK
- Encryption: TKIP
- WEP key: 0123456789

The following registry keys and registry values control the behavior of the three controllable APs:

HKEY_CURRENT_USER\Software\Microsoft\CETest\APCTL\AP1

| Value | Type | Description |
|---------------------|--------|-------------------|
| SSID | REG_SZ | WIFI_OPEN1 |
| Configurator | REG_SZ | dlink; 10.10.0.46 |
| Attenuator | REG_SZ | Manual; 0,0,100 |

HKEY_CURRENT_USER\Software\Microsoft\CETest\APCTL\AP2

| Value | Type | Description |
|---------------------|--------|---------------------------------|
| SSID | REG_SZ | WIFI_OPEN2 |
| Configurator | REG_SZ | buffalo; 10.10.0.47:admin:admin |
| Attenuator | REG_SZ | Manual; 0,0,100 |

HKEY_CURRENT_USER\Software\Microsoft\CETest\APCTL\AP3

| Value | Type | Description |
|---------------------|--------|---|
| SSID | REG_SZ | WIFI_OPEN3 |
| Configurator | REG_SZ | dlink; 10.10.0.48:dlinkroot:dlinkpasswd |
| Attenuator | REG_SZ | Manual; 0,0,100 |

At a command prompt on the server, run the following command:

```
apcontrol.exe -v -z -k Software\Microsoft\CETest\APCTL
```

At a command prompt on the device, run the following command:

```
\Windows\tux.exe -f\temp\amdebug.log -d authmatrix.dll  
-c "-lHost 10.10.0.2"
```

See Also

Tasks

[Running the Wi-Fi Authentication Tests](#)

Other Resources

[Wi-Fi Authentication Tests](#)

Command Line Parameters for the Wi-Fi Authentication Tests



8/27/2008

The Wi-Fi Authentication Tests run from the command line. The combination of authentication and encryption in each test depend on the command-line parameters you include when you start the test. To simplify the description of the parameters, this topic describes one of the parameters and links to other topics that describe the rest of the parameters.

Syntax

[Copy Code](#)

```
tux.exe [tuxparams] -d authmatrix.dll [-c "[-adapter adapterName] [apParameters] [enrollmentParameters] [logonParameters] [miscParameters]"]
```

Command-Line Parameters

tux.exe *tuxparams*

For information about the command-line parameters of the Tux test harness, see [Tux Command-Line Parameters](#).

-d authmatrix.dll

Specifies the DLL to use for the Wi-Fi Authentication Tests.

-c " ... "

Specifies a list of test-specific parameters that Tux passes to the test DLL.

-adapter adapterName

Specifies the name of the wireless adapter to use in the test. If you omit this parameter, the test uses the first wireless adapter it finds.

apParameters

Specifies the AP Control Server by hostname and port. For more information, see [AP Control Server Settings for the Wi-Fi Authentication Tests](#).

enrollmentParameters

Specifies how the AP Control application, APControl.exe, reaches the authentication server, and how to run the certificate enrollment program. For more information, see [Certificate Enrollment Settings for the Wi-Fi Authentication Tests](#).

logonParameters

Specifies how the application should interact with the user-credential dialog boxes on the device. For more information, see [User Log-on Settings for the Wi-Fi Authentication Tests](#).

miscParameters

Specifies segments of the tests to skip, APs to use, logon credentials, and test iterations and timeouts. For more information, see [Authentication Test Settings for the Wi-Fi Authentication Tests](#).

See Also

Tasks

[Running the Wi-Fi Authentication Tests](#)

Reference

[Tux Command-Line Parameters](#)

Other Resources

[Wi-Fi Authentication Tests](#)

AP Control Server Settings for the Wi-Fi Authentication Tests



8/27/2008

The AP Control Server command-line parameters specify the AP Control Server to which the test should connect.

Command-Line Parameters

| Command-Line Parameter | Description |
|------------------------|--|
| -wHost | WiFi server name/address (default "10.10.0.1") |

| | |
|---------|---|
| -wPort | WiFi server port (default 33331) |
| -wSSID | WiFi server SSID (default "") |
| -wAuth | WiFi server authentication (default "Open") |
| -wEncr | WiFi server encryption-cipher (default "ClearText") |
| -wEap | WiFi server EAP auth-mode (default "TLS") |
| -wIndex | WiFi server WEP-key index (default 0) |
| -wKey | WiFi server encryption-key (default "") |

See Also

Reference

[Command Line Parameters for the Wi-Fi Authentication Tests](#)

Other Resources

[Wi-Fi Authentication Tests](#)

Certificate Enrollment Settings for the Wi-Fi Authentication Tests



8/27/2008

The following table shows the certificate enrollment command line parameters for the Wi-Fi Authentication Matrix Test.

If the EAP tests are enabled, the first test automatically retrieves certificates for authenticating EAP connections. The certificate enrollment settings tell the test application how to reach the authentication server and how to run the certificate enrollment program.

Command-Line Parameters

| Parameter | Description |
|----------------------------------|--|
| -nHost <i>hostName</i> | Specifies the enrollment host name or address. The default value of <i>hostName</i> is 10.10.0.1. |
| -nCommand <i>cmd</i> | Specifies the enrollment host command name. The default value of <i>cmd</i> is <code>enroll</code> . |
| -nRootBox <i>title</i> | Specifies the title of the set root cert dialog box. The default value of <i>title</i> is Root Certificate Store. |
| -nToolBox <i>title</i> | Specifies the title of the "insert new cert" dialog box. The default value of <i>title</i> is Enrollment Tool. |
| -nWaitTime <i>time</i> | Specifies the time in milliseconds to wait for command. The default value of <i>time</i> is 900000, which equals 15 minutes. |

See Also

Reference

[Command Line Parameters for the Wi-Fi Authentication Tests](#)

Other Resources

[Wi-Fi Authentication Tests](#)

User Log-on Settings for the Wi-Fi Authentication Tests



8/27/2008

Each time a Wi-Fi Authentication test connects using WEP 802.1X, WPA or WPA2, the test must authenticate with the RADIUS server. The user logon settings specify how the application should interact with the user-credentials dialogs on the device. You rarely need to specify these test parameters because the test application usually provides the credentials directly, so the dialogs are not normally used, and the defaults are usually appropriate.

Command-Line Parameters

| Command-Line Parameter | Description |
|-------------------------------|--|
| -uUsrBox <i>name</i> | Specifies the title of the user logon dialog box. The default value is <code>User Logon</code> . |
| -uNetBox <i>title</i> | Specifies the title of the network password dialog box. The default value of <i>title</i> is <code>Enter Network Password</code> . |
| -uWaitTime <i>time</i> | Specifies the time in milliseconds to wait for the dialog to close. The default value of <i>time</i> is <code>300000</code> , which equals five minutes. |

See Also

Reference

[Command Line Parameters for the Wi-Fi Authentication Tests](#)

Other Resources

[Wi-Fi Authentication Tests](#)

Authentication Test Settings for the Wi-Fi Authentication Tests



8/27/2008

The Wi-Fi Authentication Tests support command-line parameters that specify segments of the tests to skip, APs to use, logon credentials, and test iterations and timeouts.

Command-Line Parameters

| Parameter | Description |
|--|--|
| -dOpen | Disables (skips) Open System (no authentication) tests |
| -dShared | Disables Shared (WEP authentication) tests |
| -d802 | Disables 802.1X (dynamic WEP) tests |
| -dEAP | Disables EAP (RADIUS) tests (WEP 802.1X, WPA and WPA2) |
| -dPSK | Disables PSK tests (WPA-PSK and WPA2-PSK) |
| -dWPA2 | Disables WPA2 tests (AES, WPA2 and WPA2-PSK) |
| -dClear | Disables ClearText (no encryption) tests |
| -dWEP | Disables WEP encryption tests |
| -dTKIP | Disables TKIP encryption tests |
| -dAES | Disables AES encryption tests |
| -dPEAP | Disables PEAP EAP-authentication tests |
| -dTLS | Disables TLS EAP-authentication tests |
| -tAPNames <i>name1,name2,...</i> | Specifies a comma-separated list of access point (AP) names. Normally, the test selects from among all the APs controlled by the AP control server. The -tAPNames parameter forces the application to select from the listed APs. If the list contains multiple AP names, the tests applies the following rules to choose the AP: |

| | |
|-------------------------------|--|
| | <ol style="list-style-type: none"> 1. If an AP has a matching security mode, use it. 2. Else, if not all the APs support the security modes, use the first that does support the mode. 3. Else, use the first AP in the list. |
| -ITLS <i>tlsCred</i> | Specifies the TLS login credentials in the format <i>user_name:password:domain_name</i> . The default value of <i>tlsCred</i> is <code>eaptls:eaptls:wince</code> . |
| -IPEAP <i>peapCred</i> | Specifies the PEAP login credentials in the format <i>user_name:password:domain_name</i> . The default value of <i>peapCred</i> is <code>eappeap:eappeap:wince</code> . |
| -tPasses <i>num</i> | Specifies the number of times to repeat each connection. The default value of <i>num</i> is 1. |
| -tConnTime <i>time</i> | Specifies the time in seconds to await a connection. The default value of <i>time</i> is 140. |

See Also

Reference

[Command Line Parameters for the Wi-Fi Authentication Tests](#)

Other Resources

[Wi-Fi Authentication Tests](#)

Test Cases for the Wi-Fi Authentication Test



8/27/2008

The topics in this section describe the test cases for the Wi-Fi Authentication tests.

In This Section

[Open Authentication Test Cases](#)

Provides a list of the test cases for wireless connections with open authentication.

[Shared Authentication Test Cases](#)

Provides a list of the test cases for wireless connections with shared authentication.

[WEP 802.1x Authentication Test Cases](#)

Provides a list of the test cases for wireless connections with WEP 802.1x authentication.

[WPA Authentication Test Cases](#)

Provides a list of the test cases for wireless connections with WPA authentication.

[WPA-PSK Authentication Test Cases](#)

Provides a list of the test cases for wireless connections with WPA-PSK authentication.

[WPA2 Authentication Test Cases](#)

Provides a list of the test cases for wireless connections with WPA2 authentication.

[WPA2-PSK Authentication Test Cases](#)

Provides a list of the test cases for wireless connections with WPA2-PSK authentication.

See Also

Other Resources

[Wi-Fi Authentication Tests](#)

Open Authentication Test Cases

Writing Sample--Windows Mobile Wireless Tests—"After" Example
Katy Koenen



8/27/2008

The following table shows the open authentication tests included in the Wi-Fi Authentication Tests.

| Test case | Description |
|-----------|--|
| 2000 | Auth=Open; Cipher=ClearText |
| 2100 | Auth=Open; Cipher=WEP 40-bit key (random) |
| 2110 | Auth=Open; Cipher=WEP 40-bit key (semi-null) |
| 2120 | Auth=Open; Cipher=WEP 40-bit key (semi-ones) |
| 2130 | Auth=Open; Cipher=WEP 104-bit key (random) |
| 2140 | Auth=Open; Cipher=WEP 104-bit key (semi-null) |
| 2150 | Auth=Open; Cipher=WEP 104-bit key (semi-ones) |
| 2200 | This test case should fail AP: Auth=Open, Cipher=WEP; STA: Auth=Open, Cipher=TKIP |
| 2300 | This test case should fail AP: Auth=Open, Cipher=WEP; STA: Auth=Open, Cipher=AES |

See Also

Other Resources

[Test Cases for the Wi-Fi Authentication Test](#)

[Wi-Fi Authentication Tests](#)

Shared Authentication Test Cases



8/27/2008

The following table shows the shared authentication tests included in the Wi-Fi Authentication Tests.

| Test case | Description |
|-----------|--|
| 3000 | This test case should fail AP: Auth=Shared Cipher=WEP; STA: Auth=Shared, Cipher=ClearText |
| 3100 | Auth=Shared; Cipher=WEP 40-bit key (random) |
| 3110 | Auth=Shared; Cipher=WEP 40-bit key (semi-null) |
| 3120 | Auth=Shared; Cipher=WEP 40-bit key (semi-ones) |
| 3130 | Auth=Shared; Cipher=WEP 104-bit key (random) |
| 3140 | Auth=Shared; Cipher=WEP 104-bit key (random) |
| 3150 | Auth=Shared; Cipher=WEP 104-bit key (semi-ones) |
| 3200 | This test case should fail AP: Auth=Shared, Cipher=WEP; STA: Auth=Shared, Cipher=TKIP |
| 3300 | This test case should fail AP: Auth=Shared, Cipher=WEP; STA: Auth=Shared, Cipher=AES |

See Also

Other Resources

[Test Cases for the Wi-Fi Authentication Test](#)

[Wi-Fi Authentication Tests](#)

WEP 802.1x Authentication Test Cases



8/27/2008

The following table shows the WEP 802.1x authentication tests included in the Wi-Fi Authentication Tests.

| Test case | Description |
|-----------|--|
| 4000 | This test case should fail AP: Auth=WEP_802_1X, Cipher=WEP; STA: Auth=WEP_802_1X Cipher=ClearText |
| 4100 | Auth=WEP_802_1X; Cipher=WEP EAP=TLS |
| 4120 | Auth=WEP_802_1X; Cipher=WEP EAP=PEAP |
| 4200 | This test case should fail AP: Auth=WEP_802_1X, Cipher=WEP; STA: Auth=WEP_802_1X, Cipher=TKIP |
| 4300 | This test case should fail AP: Auth=WEP_802_1X, Cipher=WEP; STA: Auth=WEP_802_1X, Cipher=AES |

See Also

Other Resources

[Test Cases for the Wi-Fi Authentication Test](#)

[Wi-Fi Authentication Tests](#)

WPA Authentication Test Cases



8/27/2008

The following table shows the WPA authentication tests included in the Wi-Fi Authentication Tests.

| Test case | Description |
|-----------|--|
| 5000 | This test case should fail AP: Auth=WPA, Cipher=TKIP; STA: Auth=WPA, Cipher=ClearText |
| 5100 | This test case should fail AP: Auth=WPA, Cipher=TKIP; STA: Auth=WPA, Cipher=WEP |
| 5200 | Auth=WPA; Cipher=TKIP EAP=TLS |
| 5220 | Auth=WPA; Cipher=TKIP EAP=PEAP |
| 5300 | Auth=WPA; Cipher=AES EAP=TLS |

See Also

Other Resources

[Test Cases for the Wi-Fi Authentication Test](#)

[Wi-Fi Authentication Tests](#)

WPA-PSK Authentication Test Cases



Writing Sample--Windows Mobile Wireless Tests—"After" Example
Katy Koenen

The following table shows the WPA-PSK authentication tests included in the Wi-Fi Authentication Tests.

| Test case | Description |
|-----------|--|
| 6000 | This test case should fail AP: Auth=WPA_PSK, Cipher=TKIP; STA: Auth=WPA_PSK, Cipher=ClearText |
| 6100 | This test case should fail AP: Auth=WPA_PSK, Cipher=TKIP; STA: Auth=WPA_PSK, Cipher=WEP |
| 6200 | Auth=WPA_PSK; Cipher=TKIP 63-digit passphrase (random) |
| 6210 | Auth=WPA_PSK; Cipher=TKIP 8-digit passphrase (random) |
| 6220 | This test case should fail Auth=WPA_PSK; Cipher=TKIP 7-digit passphrase |
| 6230 | Auth=WPA_PSK; Cipher=TKIP 63-digit passphrase (semi-ones) |
| 6240 | Auth=WPA_PSK; Cipher=TKIP 8-digit passphrase (semi-ones) |
| 6250 | This test case should fail Auth=WPA_PSK; Cipher=TKIP 64-digit passphrase |
| 6260 | Auth=WPA_PSK; Cipher=TKIP 63-digit passphrase (semi-null) |
| 6270 | Auth=WPA_PSK; Cipher=TKIP 8-digit passphrase (semi-null) |
| 6300 | Auth=WPA_PSK; Cipher=AES 63-digit passphrase (random) |
| 6310 | Auth=WPA_PSK; Cipher=AES 8-digit passphrase (random) |
| 6320 | This test case should fail Auth=WPA_PSK; Cipher=AES 7-digit passphrase |
| 6330 | Auth=WPA_PSK; Cipher=AES 63-digit passphrase (semi-ones) |
| 6340 | Auth=WPA_PSK; Cipher=AES 8-digit passphrase (semi-ones) |
| 6350 | This test case should fail Auth=WPA_PSK; Cipher=AES 64-digit passphrase |
| 6360 | Auth=WPA_PSK; Cipher=AES 63-digit passphrase (semi-null) |
| 6370 | Auth=WPA_PSK; Cipher=AES 8-digit passphrase (semi-null) |

See Also

Other Resources

[Test Cases for the Wi-Fi Authentication Test](#)

[Wi-Fi Authentication Tests](#)

WPA2 Authentication Test Cases



Windows Mobile



Windows Embedded CE

The following table shows the WPA2-PSK authentication tests included in the Wi-Fi Authentication Tests.

| Test case | Description |
|-----------|--|
| 7000 | This test case should fail AP: Auth=WPA2, Cipher=TKIP; STA: Auth=WPA2, Cipher=ClearText |
| 7100 | This test case should fail |

| | |
|------|--|
| | AP: Auth=WPA2, Cipher=TKIP; STA: Auth=WPA2, Cipher=WEP |
| 7200 | Auth=WPA2; Cipher=TKIP EAP=TLS |
| 7220 | Auth=WPA2; Cipher=TKIP EAP=PEAP |
| 7300 | Auth=WPA2; Cipher=AES EAP=TLS |
| 7320 | Auth=WPA2; Cipher=AES EAP=PEAP |

See Also

Other Resources

[Test Cases for the Wi-Fi Authentication Test](#)

[Wi-Fi Authentication Tests](#)

WPA2-PSK Authentication Test Cases



8/27/2008

The following table shows the WPA-PSK authentication tests included in the Wi-Fi Authentication Tests.

| Test case | Description |
|-----------|---|
| 8000 | This test case should fail AP: Auth=WPA2_PSK, Cipher=TKIP; STA: Auth=WPA2_PSK, Cipher=ClearText. |
| 8100 | This test case should fail AP: Auth=WPA2_PSK, Cipher=TKIP; STA: Auth=WPA2_PSK, Cipher=ClearText. |
| 8200 | Auth=WPA2_PSK; Cipher=TKIP 63-digit pass phrase (random) |
| 8210 | Auth=WPA2_PSK; Cipher=TKIP 8-digit pass phrase (random) |
| 8220 | This test case should fail Auth=WPA2_PSK; Cipher=TKIP 7-digit pass phrase |
| 8230 | Auth=WPA2_PSK; Cipher=TKIP 63-digit pass phrase (semi-ones) |
| 8240 | Auth=WPA2_PSK; Cipher=TKIP 8-digit pass phrase (semi-ones) |
| 8250 | This test case should fail Auth=WPA2_PSK; Cipher=TKIP 64-digit pass phrase |
| 8260 | Auth=WPA2_PSK; Cipher=TKIP 63-digit pass phrase (semi-null) |
| 8270 | Auth=WPA2_PSK; Cipher=TKIP 8-digit pass phrase (semi-null) |
| 8300 | Auth=WPA2_PSK; Cipher=AES 63-digit pass phrase (random) |
| 8310 | Auth=WPA2_PSK; Cipher=AES 8-digit pass phrase (random) |
| 8320 | This test case should fail Auth=WPA2_PSK; Cipher=AES 7-digit pass phrase |
| 8330 | Auth=WPA2_PSK; Cipher=AES 63-digit pass phrase (semi-ones) |
| 8340 | Auth=WPA2_PSK; Cipher=AES 8-digit pass phrase (semi-ones) |
| 8350 | This test case should fail Auth=WPA2_PSK; Cipher=AES 64-digit pass phrase |
| 8360 | Auth=WPA2_PSK; Cipher=AES 63-digit pass phrase (semi-null) |
| 8370 | Auth=WPA2_PSK; Cipher=AES 8-digit pass phrase (semi-null) |

See Also

Other Resources

[Test Cases for the Wi-Fi Authentication Test](#)

[Wi-Fi Authentication Tests](#)

Troubleshooting the Wi-Fi Authentication Tests



8/27/2008

Test cases 2200, 2300, 3000, 3200, 3300, 4000, 4200, 4300, 5000, 5100, 6000, 6100, 6220, 6250, 6320, 6350, 7000, 7100, 8000, 8100, 8220, 8250, 8320, and 8350 are expected to fail, because they intentionally provide incorrect information to make sure that the authentication fails when it should. Since these failures are normal, the test cases will return a **PASSED** value when the invalid association attempts fail.

For more troubleshooting help, see [Troubleshooting the CETK Tests](#).

See Also

Other Resources

[Wi-Fi Authentication Tests](#)